



# **FortiAnalyzer 6.2**

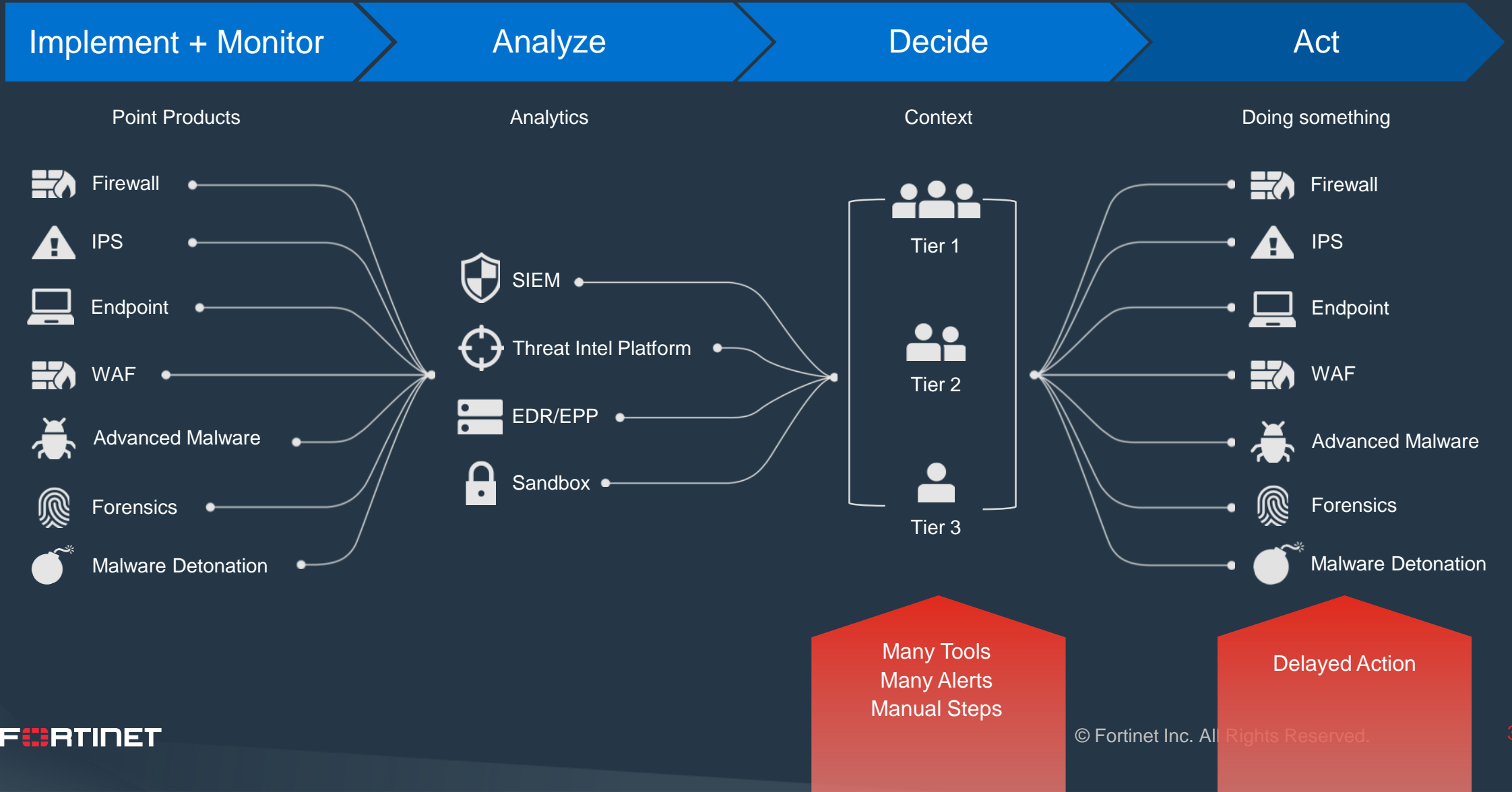
## **Incident Response & SOC Automation**

Roland Stierli

# In this session you will learn

- 1 6.2 Highlights
- 2 FortiAnalyzer-Cloud & Licensing
- 3 FAZ Positioning, Sizing & Deployment Use Cases

# Enterprise Operations



# Incident Response & Automation



## INCIDENT RESPONSE

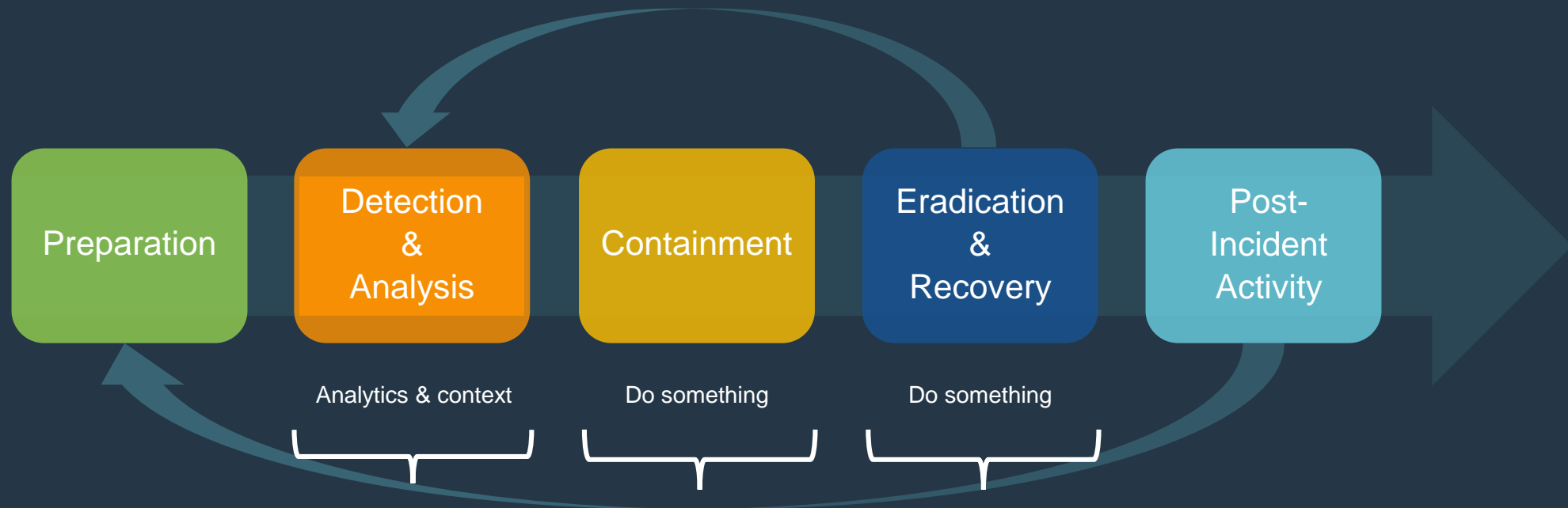
Enabling quick detection, automated correlation and connected remediation



## SOC AUTOMATION

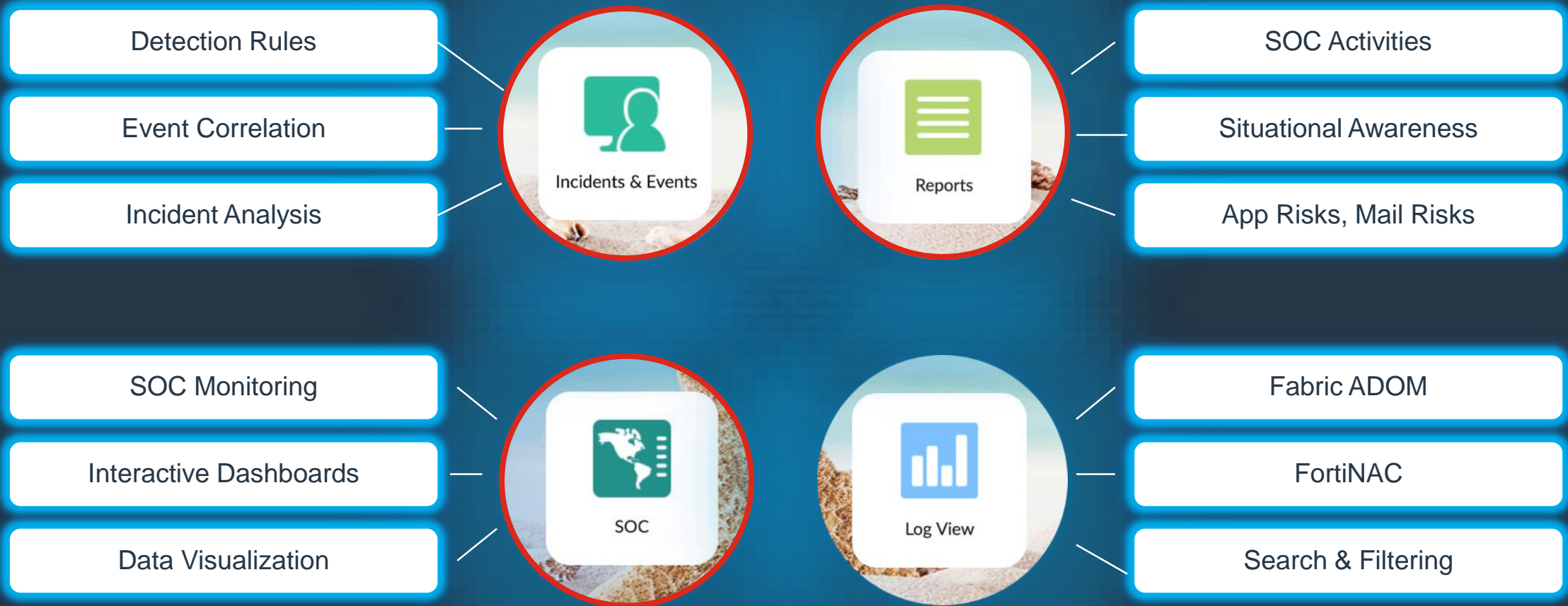
Automating manual, time-consuming processes (end-to-end) to offload SOC

# Incident Response Process



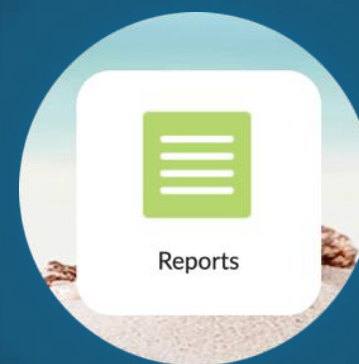
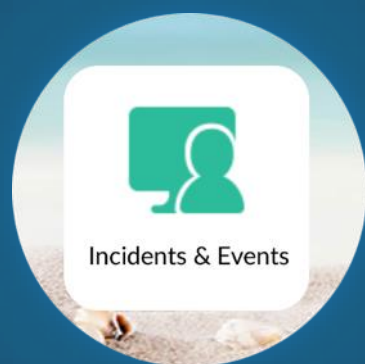
Incident Response Process (NIST 800-61r2)

# What's New In 6.2?



Find out more: Go to FNDN FortiDemo: <https://fndn.fortinet.net/index.php?/fortidemo/instances/>

# Incident Detection & Analysis



Incidents & Events

Event Monitor

All Devices • Last 7 Days • Expand All Show Acknowledged Refresh

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags
1	148.81.111.1...	Unresolved	Traffic	86	Critical	A day ago	A few seconds ago	Default-Comp...	IP: C&C	
2	176.31.42.76...	Unresolved	Traffic	86	Critical	A day ago	A few seconds ago	Default-Comp...	IP: C&C	
3	Address M...	Unresolved	Traffic	12	Critical	A day ago	A few seconds ago	Default-Comp...	IP: C&C	
4	23.253.46.64...	Unresolved	Traffic	83	Critical	A day ago	A few seconds ago	Default-Comp...	IP: C&C	
5	Enterprise_C...	Event	Event	34	Critical	A day ago	A few seconds ago	Default-FOS Sys...	System	
6	Enterprise_C...	Mitigated	DNS	10	Medium	A day ago	A few seconds ago	DomainIndexall...	Risky Dom...	
7	Glen Moh...	Mitigated	DNS	10	Medium	A day ago	A few seconds ago	DomainIndexall...	Risky Dom...	
8	Glen Moh...	Unresolved	Traffic	12	Critical	A day ago	A few seconds ago	Default-Comp...	C&C IP	
9	MS348.Serv...	Mitigated	IPS	696	Medium	A day ago	A minute ago	Default-Malici...	Intrusion	Sig...
10	10.100.77.35...	Mitigated	IPS	336	Medium	A day ago	A minute ago	Default-Malici...	Intrusion	Sig...
11	Lane Dom...	Mitigated	IPS	363	Medium	A day ago	A minute ago	Default-Malici...	Intrusion	Sig...
12	Kerry Bates...	Unresolved	Traffic	12	Critical	A day ago	A minute ago	Default-Comp...	C&C IP	
13	70.15.236.24...	Unresolved	Traffic	586	Critical	A day ago	A minute ago	Default-Comp...	IP: C&C	
14	Riley Monah...	Unresolved	Traffic	11	Critical	A day ago	A minute ago	Default-Comp...	C&C IP	
15	187.188.83.5...	Unresolved	Traffic	609	Critical	A day ago	A minute ago	Default-Comp...	IP: C&C	
16	Jesse Hugh...	Unresolved	Traffic	12	Critical	A day ago	A minute ago	Default-Comp...	C&C IP	
17	Enterprise_S...	Event	Event	25	Critical	A day ago	2 minutes ago	Default-FOS Sys...	System	
18	84777920.g42...	Mitigated	DNS	968	Medium	A day ago	2 minutes ago	Default-Risky-D...	Risky Dom...	
19	84777920.g42...	Mitigated	DNS	968	Medium	A day ago	2 minutes ago	Default-Risky-D...	Risky Dom...	
20	Glen Morgan...	Mitigated	DNS	19	Medium	A day ago	2 minutes ago	Default-Risky-D...	Risky Dom...	
21	Lane Ramon...	Unresolved	Traffic	12	Critical	A day ago	2 minutes ago	Default-Comp...	C&C IP	
22	84777920.g42...	Mitigated	DNS	968	Medium	A day ago	2 minutes ago	Default-Risky-D...	Risky Dom...	
23	Caden Dorsey...	Mitigated	DNS	19	Medium	A day ago	2 minutes ago	Default-Comp...	C&C IP	
24	recruiteme...	Mitigated	DNS	968	Medium	A day ago	2 minutes ago	Default-Risky-D...	Risky Dom...	
25	84777920.g42...	Unresolved	Traffic	12	Critical	A day ago	2 minutes ago	Default-Comp...	C&C IP	

SOC FortiView Monitors

Dashboard • All Devices • Last 1 Hour • 13:44:04 • Refresh Day Night Ocean

Threats

Top Threats

Threat Map

Compromised Hosts

FortiGuard Detection

Traffic

Applications & Websites

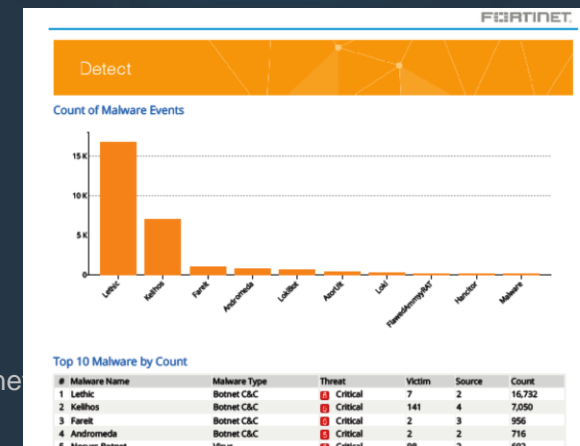
VPN

System

#	End User	Last Detected	Host Name	OS	Verdict	# of Threats	Device Name
1	Daniil Dominguez 10.200.1.15	05/28/2019 02:44	Daniil Dominguez Desktop	@Mac OS X	Infected	2	Enterprise_Core
2	Kir Kennedy 10.200.1.14	05/28/2019 02:43	Kir Kennedy PC	@Linux LIBUNTY	Infected	2	Enterprise_Core
3	Eli Bailey 10.200.1.13	05/28/2019 02:43	Eli Bailey Laptop	@Mac OS X	Infected	2	Enterprise_Core
4	Willy Fox 10.200.1.12	05/28/2019 02:43	Willy Fox Laptop	@Linux LIBUNTY	Infected	2	Enterprise_Core
5	Caden Dorsey 10.100.92.15	05/28/2019 02:42	Caden Dorsey Desktop	@Linux LIBUNTY	Infected	2	Enterprise_Core
6	Sam Key 10.200.1.11	05/28/2019 02:42	Sam Key PC	@Linux LIBUNTY	Infected	2	Enterprise_Core
7	Kerry Robinson 10.100.91.5	05/28/2019 02:42	Kerry Robinson Laptop	@Linux LIBUNTY	Infected	1	Enterprise_First_Floor
8	Styler Price 10.200.1.10	05/28/2019 02:42	Styler Price PC	@Mac OS X	Infected	2	Enterprise_Core
9	Kal Stevens 10.200.1.9	05/28/2019 02:42	Kal Stevens Laptop	@Linux LIBUNTY	Infected	2	Enterprise_Core
10	Eli Kennedy 10.200.1.8	05/28/2019 02:41	Eli Kennedy PC	@Linux LIBUNTY	Infected	2	Enterprise_Core
11	Shay Roman 10.200.1.7	05/28/2019 02:41	10.200.1.7	@Mac OS X	Infected	2	Enterprise_Core
12	Gale Clarke 10.200.1.6	05/28/2019 02:40	Gale Clarke Laptop	@Mac OS X	Infected	2	Enterprise_Core
13	Riley Monahan 10.100.91.17	05/28/2019 02:40	Riley Monahan Desktop	@Mac OS X	Infected	2	Enterprise_Core
14	Sidney Carr 10.200.1.5	05/28/2019 02:40	Sidney Carr Laptop	@Linux LIBUNTY	Infected	2	Enterprise_Core
15	Kir Thompson 10.200.1.4	05/28/2019 02:40	Kir Thompson Desktop	@Linux LIBUNTY	Infected	2	Enterprise_Core
16	Justice Foster 10.200.1.3	05/28/2019 02:39	Justice Foster Laptop	@Mac OS X	Infected	2	Enterprise_Core
17	Jo Ayala 10.200.1.2	05/28/2019 02:39	Jo Ayala PC	@Linux LIBUNTY	Infected	2	Enterprise_Core
18	Adrian Medina 10.200.1.21	05/28/2019 02:39	Adrian Medina PC	@Mac OS X	Infected	2	Enterprise_Core
19	Glen Wallace 10.200.1.20	05/28/2019 02:38	Glen Wallace Desktop	@Mac OS X	Infected	2	Enterprise_Core
20	Kerry Bates 10.200.1.19	05/28/2019 02:38	Kerry Bates Desktop	@Linux LIBUNTY	Infected	2	Enterprise_Core
21	Jesse Hughes 10.200.1.18	05/28/2019 02:38	Jesse Hughes Desktop	@Linux LIBUNTY	Infected	2	Enterprise_Core

Show 100 • Total 23

© Fortinet



# Incident Detection & Analysis – IOC History Scan

The screenshot displays the FortiView Monitors interface. The left sidebar shows navigation options: Threats, Top Threats, Threat Map, Compromised Hosts (selected), FortiSandbox Detection, Traffic, Applications & Websites, VPN, and System. The main panel is titled 'Compromised Hosts' and shows a table of hosts. A dialog box titled 'Edit IOC Rescan Policy Settings' is open, showing rescan tasks and global settings.

**Compromised Hosts Table:**

#	Host	Status	Threat Count	Log Count	Package Update Time	New Blacklist Count
18	Eli Bailey( 10.200.1. 04/05/2019 02:34	Infected	2			

**Edit IOC Rescan Policy Settings Dialog:**

**Rescan tasks**

Start Time	Status	Percentage	End Time	Threat Count	Log Count	Package Update Time	New Blacklist Count
Nov 04 15:00:01	complete	100%	Nov 04 15:14:26	1	414119883	Nov 04 13:37:44	309
Nov 03 15:00:00	complete	100%	Nov 03 15:14:19	1	415022561	Nov 03 13:37:20	2673
Nov 02 15:00:01	complete	100%	Nov 02 15:13:31	1	415022561	Nov 02 14:02:10	283
Nov 02 10:16:19	complete	100%	Nov 02 10:31:12	799	415022561	Nov 02 10:14:08	3

**IOC Rescan Global Settings**

- Enable Global IOC Rescan: ☒
- Running at: 3:00:00 PM

**IOC Rescan Current Adom Settings**

- Enable Current Adom IOC Rescan: ☒
- Log Type Filters: ☒ DNS logs, ☒ Web filter logs, ☒ Traffic logs
- Last N Days: 30

Buttons: OK, Cancel

Find out more about IOC: <https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/779346/how-ioc-works>



# Incident Analysis – Threat Intel Lookup

[Home](#) / [FAQ](#) / [IOC Form](#)

## At a glance:

If you believe the supplied IP address, domain or URL is not correctly classified, enter your comments and submit the IP address, domain or URL for review using this form.

## Indicator of Compromise Form

### IP/Domain/URL



Enter an IP address, url or domain be re-evaluated

### Category

- False Positive
- ✓ Confirmed IOC
- Suspicious



### Contact Information

Name

Email

# Incident Analysis – Timeline and Life Cycle

Incidents & Events

Event Monitor

All Events

By Endpoint

By Threat

System Events

Event Handler List

Subnet List

Incidents

All Incidents

Incident Settings

FortiGate Event Handlers

IN00000044 2019-04-05 17:55:29

Affected Endpoint and User

Topology

Addresses

Operating System

Incident Life Cycle

From 2019-04-05 05:55:29 To 2019-04-05 06:08:36

New

Analysis

Response

Incident Info

Incident Reporter

Incident Category

Severity

Status

Description

Timeline

From 2019-04-05 16:09:41 To 2019-04-05 17:51:03 (Total 12 Events)

15:00

15:15

15:30

15:45

16:00

16:15

16:30

16:45

17:00

17:15

17:30

17:45

18:00

18:15

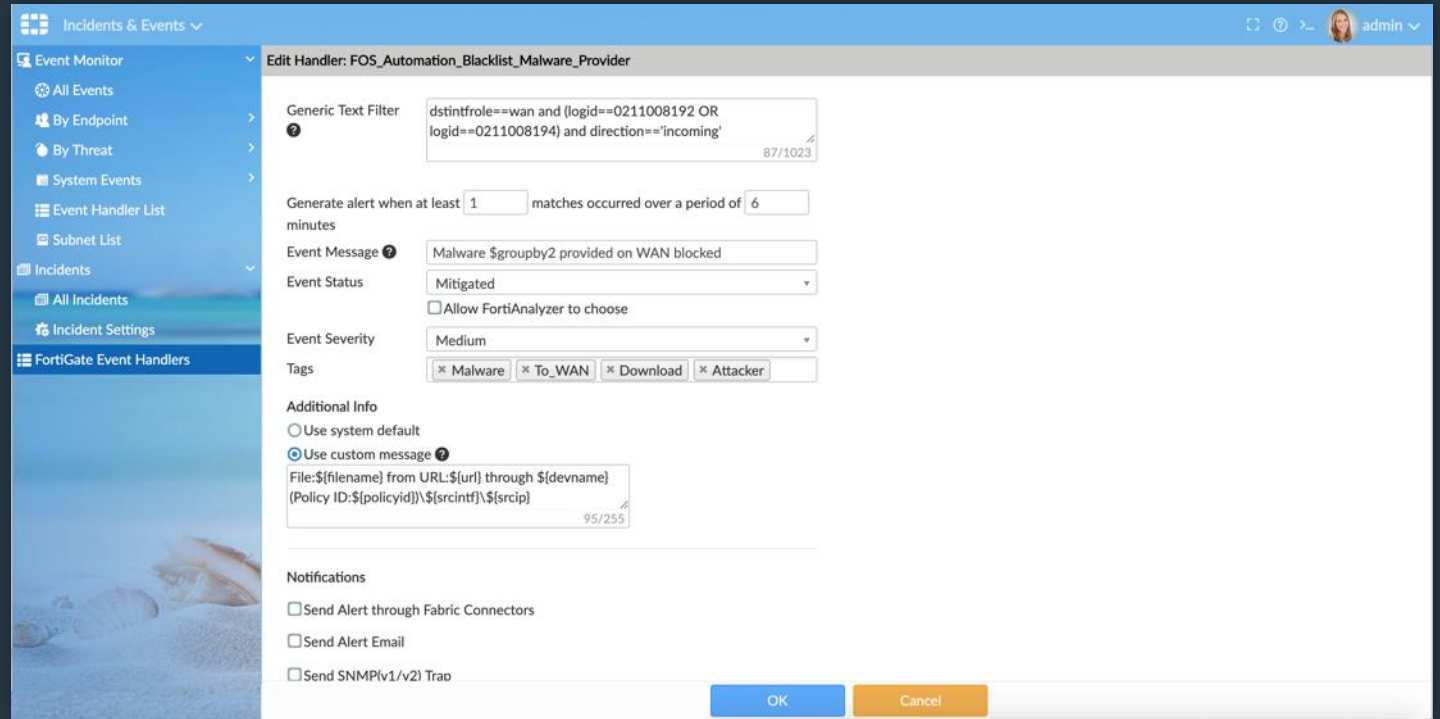
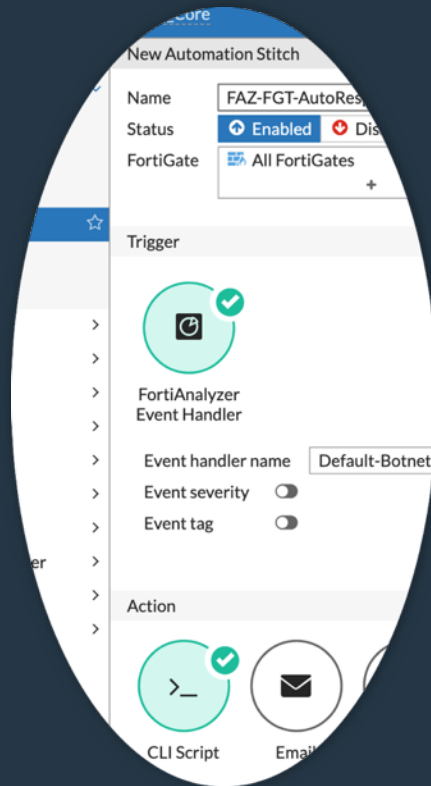
18:30

Events

Delete

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags
1	Malware VBA/Ag...	Mitigated	Antivirus	11	Medium	2019-04-05 16:09:41	2019-04-05 16:56:50	File:readme.txt from ...	Default-Malicious-Fil...	MalwareTo_WANDo...
2	DNS traffic to Bot...	Unhandled	DNS	22	High	2019-04-05 16:09:42	2019-04-05 16:56:49	Traffic path: Enterpris...	Default-Botnet-Com...	BotnetDomainC&C
3	Compromised hos...	Unhandled	DNS	22	Critical	2019-04-05 16:09:42	2019-04-05 16:56:49	infected-domain: daic...	Default-Compromise...	C&CDomain
4	Compromised hos...	Unhandled	Web Filter	11	Critical	2019-04-05 16:09:42	2019-04-05 16:56:49	infected-domain: daic...	Default-Compromise...	C&CURL
5	Web request to M...	Mitigated	Web Filter	11	Medium	2019-04-05 16:09:42	2019-04-05 16:56:49	Domain:daicoaero.ru,...	Default-Risky-Destin...	RiskyURL
6	Internal intrusion ...	Mitigated	IPS	7	Medium	2019-04-05 16:09:42	2019-04-05 16:56:54	outgoing internal intr...	Default-Malicious-Co...	IntrusionSignatureInt...

# Automate Incident Containment (FAZ <=> FOS)






















# Automate Incident Management End-to-End with ITSM

The screenshot displays the ServiceNow interface for managing FortiManager scripts. A modal window titled "Script Creation - Step 4" is open, showing a progress bar with five steps: Basic Info, Select ADOM, Select Script, Customize Script Variable (current step), and Select Installation Targets. The "Customized Script Variables" section contains two variables: "mac" with the value "00:15:00:9a:79:51" and "desc" with the value "Quarantine Caden Madir". The "Customized Script Preview" section shows the resulting configuration script:

```
config user quarantine
config targets
edit "Service-Now"
config macs
edit 00:15:00:9a:79:51
set description "Quarantine Caden Madir's laptop"
end
```

The background interface includes a left sidebar with navigation options like "Home", "FortiAnalyzer App", and "FortiManagerV2 App". The top header shows the "service now" logo and user information.

# Incident Eradication & Recovery

Fabric View ▾ Fabric Connectors Asset & Identity					admin ▾	
fabric ▾ Last 1 Week ▾ Mar 29 2019 - Apr 05 2019 Column Settings ▾ User Display Preferences						
User	Endpoint	Hardware / OS	▼ Vulnerabilities	IP Address / FortiGate / Interface		
 Addison Medina	Addison Medina Laptop	 Linux LUBUNTU		10.100.91.2 / Enterprise_First_Floor		
	Addison Medina PC	 Mac OS X	<div><div>10</div><div>30</div><div>50</div><div>10</div></div>	10.200.1.21 / Enterprise_Second_Flo		
 Reed Allen	Reed Allen Laptop	 Linux LUBUNTU	<div><div>6</div><div>6</div><div>60</div><div>18</div></div>	10.200.1.16 / Enterprise_Second_Flo		
 Kerry Bates	Kerry Bates Desktop	 Linux LUBUNTU	<div><div>16</div><div>64</div><div>8</div></div>	10.200.1.19 / Enterprise_Second_Flo		
	Kerry Bates Laptop	 Linux LUBUNTU		10.100.94.11 / Enterprise_First_Floor		
 Willy Fox	Willy Fox Laptop	 Linux LUBUNTU	<div><div>10</div><div>60</div><div>10</div></div>	10.200.1.12 / Enterprise_Second_Flo		
 Lane Ramos	Lane Ramos Desktop	 Mac OS X	<div><div>70</div><div>7</div></div>	10.200.1.17 / Enterprise_Second_Flo		
 Jesse Hughes	Jesse Hughes Desktop	 Linux LUBUNTU	<div><div>11</div><div>44</div><div>11</div></div>	10.200.1.18 / Enterprise_Second_Flo		
 Riley McMahon	Riley McMahon Desktop	 Mac OS X	<div><div>9</div></div>			
 Aaren Chambers	Aaren Chambers Laptop	 Linux LUBUNTU	<div><div>8</div><div>2</div><div>24</div><div>4</div></div>	10.100.71.17 / Enterprise_First_Floor		
 Fran Acosta						

Vulnerability Name

Category

[Ubuntu Security Notice USN-2936-1](#) Web Client

[Ubuntu Security Notice USN-2973-1](#) Applications

[Ubuntu Security Notice USN-2993-1](#) Web Client



# Automate Incident Eradication & Recovery

Reports ▾

Generated Reports

Report Definitions ▾

All Reports

Templates

Chart Library ⓘ

Macro Library

Datasets ⓘ

Advanced ▾

Language

Output Profile

Report Calendar

Delete ⌵ Last 7 Days ▾

Order by Time Order by Name

Time Range	Devices	Status
13 - 2019/04/03	> 19 Devices	07m 42s
13 - 2019/04/03	> 54 Devices	08m 01s
		19m 59s
		07m 16s

Prepare

Prep-1 Network Topology and Prep-1.1 Device Inventory

Overview

This category provides awareness of all en view will provide total number of devices v chart of new devices discovered by month

Risk

No ability to determine physical devices or address vulnerabilities and will increase th

Recommendations

Review the new devices discovered and ve take appropriate action to remove and inv authorized devices should record IP addre department as well as if device is portable as it can be used to build a baseline and w understand the increase or decrease of de

Endpoint Devices on Network

#	Date/Time	New Devices
1	2018-11-06 20:26:27	VAN-200902-PC
2	2018-11-06 14:03:56	VAN-903503-LT
3	2018-11-05 17:46:33	win7-vm-x32

Protect

Summary of Changes

- Edit firewall.policy
- Edit switch-controller.managed-switch
- Add firewall.policy
- Add firewall.address
- Edit firewall.lppool
- Edit router.static
- Edit vpn.ipsec.phase1-interface
- Add firewall.lppool
- Add router.static
- Edit firewall.address

Change Details

#	Date/Time	User	User Int
1	2018-11-06 16:06:53	sthakkar	GUI(17)
2	2018-11-06 16:06:53	sthakkar	GUI(17)
3	2018-11-06 16:06:50	sthakkar	GUI(17)
4	2018-11-06 16:06:50	sthakkar	GUI(17)
5	2018-11-06 16:03:14	sthakkar	GUI(17)
6	2018-11-06 16:03:14	sthakkar	GUI(17)
7	2018-11-06 16:02:08	sthakkar	GUI(17)
8	2018-11-06 16:02:08	sthakkar	GUI(17)
9	2018-11-06 16:01:36	sthakkar	GUI(17)
10	2018-11-06 16:01:36	sthakkar	GUI(17)
11	2018-11-06 16:01:23	sthakkar	GUI(17)
12	2018-11-06 16:01:23	sthakkar	GUI(17)
13	2018-11-06 16:01:05	sthakkar	GUI(17)
14	2018-11-06 16:01:05	sthakkar	GUI(17)
15	2018-11-06 15:59:22	sthakkar	GUI(17)
16	2018-11-06 15:59:21	sthakkar	GUI(17)
17	2018-11-06 15:59:05	sthakkar	GUI(17)
18	2018-11-06 15:59:05	sthakkar	GUI(17)
19	2018-11-05 17:22:47	seanzhang	GUI(17)
20	2018-11-05 17:22:47	seanzhang	GUI(17)
21	2018-11-05 17:22:17	seanzhang	GUI(17)
22	2018-11-05 17:22:17	seanzhang	GUI(17)
23	2018-11-05 17:19:21	seanzhang	GUI(17)
24	2018-11-05 17:19:21	seanzhang	GUI(17)

Detect

Count of Malware Events

Top 10 Malware by Count

#	Malware Name	Mal
1	Lethic	Bot
2	Kelihos	Bot
3	Farelit	Bot
4	Andromeda	Bot
5	Necurs.Botnet	Viru
6	LokiBot	Bot
7	AzorUlt	Bot
8	Loki	Bot
9	FlawedAmmyrAT	Bot
10	Hancitor	Bot

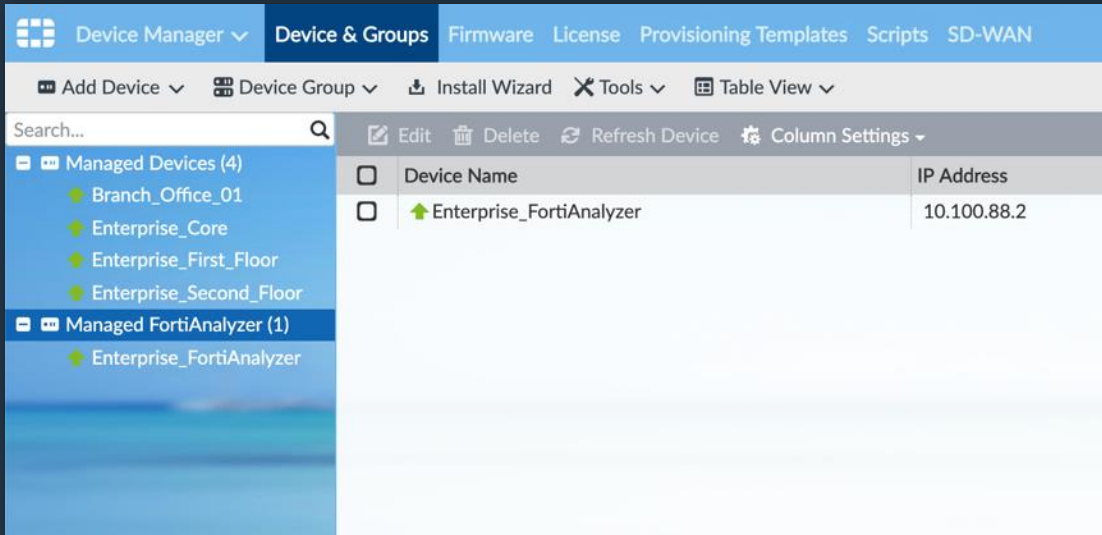
Respond & Recover

Potential Breach by Day

Top 10 Potential Breach

#	Device	#Event	Verdict	Confidence Level	Threats
1	FortinetCanadaR	8	0	817	W32/Symml,CnC
2	Android	10	0	799	CnC,Riskware/DownloaderGuide,W32/Agent,W32/Lip
3	Ikranzer-desktop	8	0	785	CnC,W32/Generic
4	dkong	4	0	658	W32/Allapple,W32/Symml
5	172.17.91.88	10	0	589	PossibleThreat,W32/Kryptik,W32/Agent,W32/Generic
6	VAN-201584-PC	6	0	548	CnC
7	DESKTOP-03TECOE	6	0	531	W32/Allapple,CnC

# Single-Pane Visibility – SOC & NOC



Device Manager ▾ Device & Groups Firmware License Provisioning Templates Scripts SD-WAN

▾ Add Device ▾ ▾ Device Group ▾ ▾ Install Wizard ✕ Tools ▾ ▾ Table View ▾

Search...

▾ Managed Devices (4)

- Branch\_Office\_01
- Enterprise\_Core
- Enterprise\_First\_Floor
- Enterprise\_Second\_Floor

▾ Managed FortiAnalyzer (1)

- Enterprise\_FortiAnalyzer

<input type="checkbox"/>	Device Name	IP Address
<input type="checkbox"/>	Enterprise_FortiAnalyzer	10.100.88.2



# Q & A



**FORTINET®**